澳門特別行政區政府
財政局

自動信息交換(AEOI)系統

金融機構用戶登入及操作手冊

版本 1.5

Website : www.dsf.gov.mo/AEOI/

版本記錄		
版本號	版本描述	版本日期
1.0	初版	08/2017
1.1	• 增加第 4 項有關測試期的 FTP 伺服器文件夾名稱 • 增加附錄二之代碼示例	09/2017
1.2	• 增加第 2 項最多可登記 3 個「高級電子簽名」證書、用戶登記的預約方式及修改所需文件的相關內容 • 增加第 4 項期限後申報的 FTP 伺服器文件夾名稱 • 修改第 4.1 項期限內申報內容 • 修改第 4.2 項期限後申報內容 • 修改第 4.3.1 項系統檢查流程內容 • 增加第 6 項證書續期安排	03/2018
1.3	• 修改第 2.1 項新登記所需文件內容	08/2018
1.4	• 修改第 1 及 1.1 項內少量用字 • 修改第 2.1 項預約電話及新增退休基金報送等說明 • 修改第 2.2 項更改資料說明 • 增加第 2.3 項「高級電子簽名」證書續期 • 修改第 3.1 項內參考資料 • 增加第 3.2 項更改登入密碼 • 修改第 4 項伺服器目錄相關說明 • 修改第 4.1 項內用字 • 增加第 4.1.1 項 期限內資料的更正 • 增加第 4.1.2 項 分拆上載 XML 檔案 • 修改第 4.2 項內用字及加入處理大量資料之描述 • 取消第 4.3.1 項並將其內容合併至第 4.1.1 項內 • 修改第 5 項標題及加入第 5.1 項標題 • 增加第 5.2 項 查閱系統內有效記錄總數 • 取消第 6 項並將其內容合併至第 2 項內	03/2022
1.5	• 修改目錄 • 更改 2.1 項內的聯絡電話	08/2023

	• 修改第 2.1, 2.2 及 2.3 項部份用字及其中一份表格名稱 • 修改第 3.2 項部份用字 • 增加第 4 項中的圖示及相關說明、並增加及更改各分項標題	

目錄

日期：2023 年 08 月

1. 簡介

財政局自動信息交換系統(以下簡稱系統)主要提供平台讓澳門各報送信息的金融機構上載有關須報送金融帳戶信息到財政局，再由系統處理及執行有關稅務信息交換工作。

1.1 文件範圍

金融機構用戶之系統操作流程，包括：

- 用戶登記；
- 登入系統；
- 上載檔案；
- 查閱報送狀態。

1.2 文件對象

- 須報送信息的金融機構

2. 用戶登記

2.1 新登記

金融機構(“由另一實體管理的投資實體[1]”除外)須先行取得郵電局 eSignTrust 發出的「高級電子簽名」證書(有關證書申請詳情，請參閱郵電局之相關網頁：http://www.esigntrust.com)，用於簽署向財政局遞交的資料檔案。如金融機構通過服務提供者報送信息，「高級電子簽名」證書須由服務提供者取得。新登記之金融機構須填妥《自動信息交換系統 – 用戶申請表》以取得系統帳戶，同一機構於財政局最多可登記 3 個「高級電子簽名」證書。

倘金融機構屬“由另一實體管理的投資實體”，另須填妥《自動信息交換系統 – 系統識別號申請表》，該等投資實體的金融帳戶信息，須透過其管理機構的系統帳戶進行報送，而 XML 檔案內之資料仍須以投資實體的名義提供，而不可使用管理機構的名義。

[1] “由另一實體管理的投資實體”是指《金融帳戶信息的通用報送標準及盡職調查程序》(“指引”)第八條第一款(七)項(2)分項的投資實體。亦即由“指引”第八條第一款內所指的存款機構、託管機構、特定保險公司或同款(七)項(1)分項所指的另一投資實體所管理的實體。

金融機構備妥上述資料後，可致電 85990799 預約辦理用戶登記手續(須提前至少 1 個工作天預約)。法定代表或其指定代辦人須按預約時間親臨財政局資源中心(地址：澳門大堂街 30 號)辦理用戶登記手續，有關帳戶可於完成手續後翌日起計第 3 個工作天使用。

2.1.1 申請手續所需文件及要求

由法定代表作申請：

1. 已完成「高級電子簽名」證書的申請手續
2. 已填妥及簽署之《自動信息交換系統 – 用戶申請表》
3. 已填妥及簽署之《自動信息交換系統 – 系統識別號申請表》(如適用)
4. 法定代表具簽名式樣之身份證明文件正本

由代辦人作申請：

1. 已完成「高級電子簽名」證書的申請手續
2. 已填妥及簽署之《自動信息交換系統 – 用戶申請表》
3. 如屬新登記或重設密碼，須同時遞交已填妥及簽署之《聲明書》
4. 已填妥及簽署之《自動信息交換系統 – 系統識別號申請表》(如適用)
5. 法定代表具簽名式樣之身份證明文件正本
6. 代辦人具簽名式樣之身份證明文件正本

註：倘屬登記使用或更改服務提供者，不論由法定代表或代辦人作申請，均須遞交已填妥及簽署之《聲明書》。上述各申請表及《聲明書》可於財政局網站 www.dsf.gov.mo下載。

2.1.2 啟動帳戶及設定密碼

金融機構法定代表或代辦人經財政局工作人員核實身份後，將可取得系統的用戶帳號，並按指示隨即在財政局啟動帳戶及設定密碼。

密碼長度至少為 8 個字碼(須包含以下四種字碼類型的其中三種)：

1. 大寫字母(A 到 Z)
2. 小寫字母(a 到 z)
3. 數字(0 到 9)
4. 標點符號(～！@＃$%^&＊_－ ＋=`|\(){} [] :; “'<>，。？/)

有關系統的登入密碼最長有效期為 12 個月，並須定期更改(有效期內可於網上更改，詳情請參閱“3.2 更改登入密碼”)。如登入密碼連續 5 次輸入錯誤，有關帳戶會被暫時鎖定。

2.2 更新資料

倘新增、更改或取消資料，金融機構須填妥對應之申請表，由法定代表或代辦人親臨財政局辦理，相關手續及其他所需文件可參閱"2.1 新登記"。倘涉及「高級電子簽名」證書的資料更改，有關更改將於財政局收到申請後翌日起計的第 3 個工作天生效。

更新事項及所須填寫之表格:

更新事項	填寫表格
1. 重設密碼	《自動信息交換系統 – 用戶申請表》
2. 更改涉及「高級電子簽名」證書的電郵地址/持有人姓名(倘為證書續期或更新請參閱"2.3「高級電子簽名」證書續期或更新")	
3. 更改已登記之用戶資料或取消用戶登記	
4. 新增、更改或取消退休基金、信託或其他"由另一實體管理的投資實體"的資料	《自動信息交換系統 – 系統識別號申請表》

2.3 「高級電子簽名」證書續期或更新

由郵電局 eSignTrust 發出的「高級電子簽名」證書倘因證書過期而須辦理續期或其他原因而須更新，必須於郵電局 eSignTrust 完成有關手續後，再透過《自動信息交換系統 – 用戶申請表》內登記之任一電郵地址，通知財政局有關證書已於郵電局 eSignTrust 完成續期，財政局完成有關證書續期之更新工作後，將以電郵回覆金融機構。如證書相關的其他資料須作更改請參閱"2.2 更新資料"。

3. 登入系統

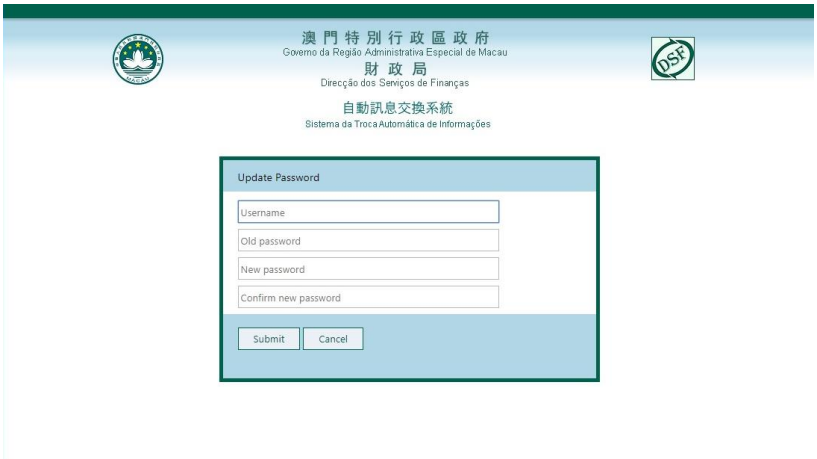
3.1 登入系統

各金融機構必須下載虛擬私人網路之軟件(VPN CLIENT)(請參閱“金融機構登入 VPN 及 FTP 客戶端用戶手冊”)。經與系統建立虛擬私人網路(SSLVPN)後，使用支援 FTPs Protocol 的軟件登入系統專用的伺服器。

註： 財政局 AEOI FTP Server 的系統時間以 UTC+08:00 作標準，並設定系統維護時間由 00:00 至 08:00，期間系統將不接受用戶登入及上載資料等操作。

3.2 更改登入密碼

建立虛擬私人網路後，金融機構可通過以下網址更改系統的登入密碼，新密碼有效期為 12 個月：
https://account.dsf－info－ex.gov.mo/

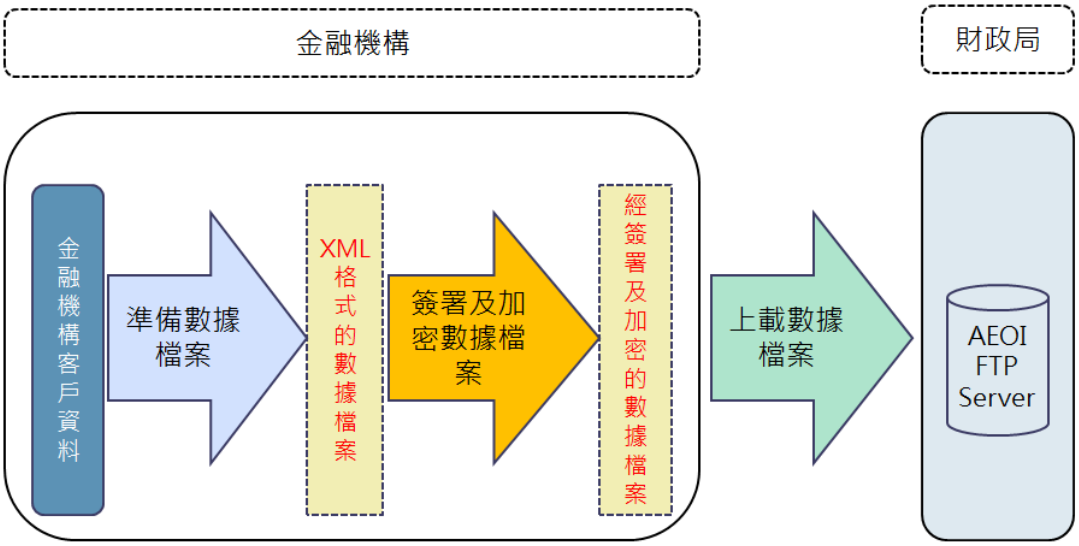


註：倘若遺失、忘記密碼或有關密碼已失效，金融機構仍須親臨財政局辦理重設密碼手續，詳情可參閱“2.2 更新資料”。

4. 上載檔案

4.1 上載檔案流程

金融機構將有關資料生成 XML 格式的數據檔案(詳情請參閱 AEOI XML Schema User Guide)，並完成簽署及加密後(詳見附錄一及附錄二)，通過 FTPs 軟件將有關檔案上載到系統專用伺服器。



4.2 伺服器文件夾說明

4.2.1 金融機構

金融機構須通過 FTPs 軟件將有關檔案上載到財政局伺服器，伺服器內各文件夾的說明如下：

表 1：處理正式報送資料的文件夾

用途及開放期	文件夾名稱 (見圖 1)	說明	用戶權限
正式報送 期限內資料 (每年於報送期限內開放)[註 1]	/IN_Production	報送資料檔案，只用於期限內報送的情況	Upload & Delete
	/OUT_Production	存放回覆檔案 (Status Message)、原報送檔案 (History) 及有效記錄之總數	Download Only
正式報送 期限後資料 (持續開放)	/IN_Production_After	報送資料檔案，只用於期限後報送的情況	Upload & Delete
	/OUT_Production_After	存放回覆檔案 (Status Message)、原報送檔案 (History) 及有效記錄之總數	Download Only

註 1：每年於報送期限後，IN_Production 文件夾的用戶權限將改為 Read Only。

表 2：處理測試資料的文件夾

用途及開放期	文件夾名稱 (見圖 1)	說明	用戶權限
測試於期限內 報送資料 (每年於報送期限內開放)[註 2]	/IN_Validation	報送資料檔案，只用於測試期限內報送的情況	Upload & Delete
	/OUT_Validation	存放回覆檔案 (Status Message)、原報送檔案 (History) 及有效記錄之總數	Download Only
測試於期限後 報送資料 (持續開放)	/IN_Validation_After	報送資料檔案，只用於測試期限後報送的情況	Upload & Delete
	/OUT_Validation_After	存放回覆檔案 (Status Message)、原報送檔案 (History) 及有效記錄之總數	Download Only

註 2：每年於報送期限後，IN_Validation 文件夾的用戶權限將改為 Read Only。

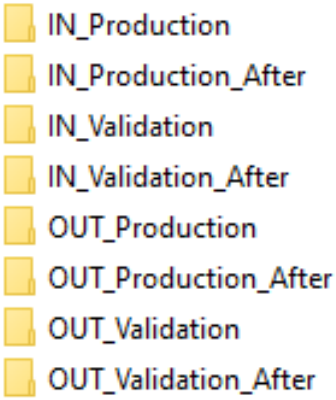


圖 1 伺服器文件夾 (圖片僅供參考，不同的 FTPs 軟件顯示方式或有所不同)

4.2.2 投資實體的管理機構

倘“管理機構”已為其管理的投資實體申請系統識別號，在登入 FTP 後，介面將先出現以各金融機構的系統識別號(AEOI ID)命名的文件夾(見圖 2)，在報送信息時需先進入對應的金融機構文件夾，再按 4.2.1 項的表 1 及表 2 文件夾說明進行報送或測試。

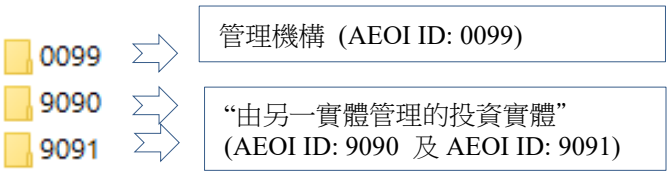


圖 2 伺服器文件夾 (圖片僅供參考，不同的 FTPs 軟件顯示方式或有所不同)

4.3 期限內報送

金融機構須最遲於每曆年的 6 月 30 日，以電子加密方式向財政局提供屬上一曆年的信息(例如：2017 年度之資料，對應之報送期為 2018 年 1 月 1 日至 2018 年 6 月 30 日)。

倘報送信息的金融機構在執行盡職調查程序後，確認其擁有的金融帳戶中並沒有須報送帳戶，則可透過公函方式通知財政局，聲明有關年度沒有須報送帳戶信息。往後年度即使上述情況維持不變，金融機構仍須每年以公函作相關聲明。

4.3.1 期限內上載完整的檔案

法定報送期內，金融機構上載的檔案須包含所有帳戶資料，且檔案名稱及格式必須符合系統要求(詳情請參閱 AEOI XML Schema User Guide)，以遞交 2017 年度的資料為例，上載的檔案名稱示例及對應處理狀態如下：

上載的檔案名稱	狀態
20170001201801201120500 0.zip	接受處理
20170001201801201120500 0.jpg	檔案名稱不正確，不作處理
2017ABC.zip	檔案名稱不正確，不作處理
20170001201801201620500 0.zip	接受處理

系統於定時執行處理程序時，會根據符合格式的檔案名稱判斷檔案的日期及時間，僅以最新的檔案作為金融機構的最近一次報送的資料。金融機構於報送期限內可多次上載完整的資料檔案，倘同一文件夾內有多個資料檔案，金融機構可自行選擇刪除無須報送的檔案，或留待系統定時執行處理程序時自動判斷最新的檔案。

4.3.2 期限內資料的更正

在報送期內，倘發現上述已報送的金融帳戶信息有誤或遺漏，金融機構可重新上載包含所有帳戶資料的檔案。

上載之檔案如符合以下三個條件，相應資料年度曾遞交的資料將被刪除(無論新上載資料有否其他錯誤)。如未能符合相關條件，先前已接受的資料將不受影響。

刪除相應資料年度曾遞交資料之條件：

1. 屬報送期限內的資料
2. 檔案名稱最後 2 位數字的序號為 00 (如: 2020019920210410112030**00**.zip)
3. 檔案通過下列檢查：

檢查內容	回覆檔案內對應的 Error Code
A. 檔案名稱	50101, 50114, 50120
B. 解壓上載資料檔	50103
C. 解密	50102, 50117, 50118
D. 解壓 XML 檔案	50116
E. 防毒檢查	50105
F. 電子簽名驗證	50104, 50119
G.資料年度	50115

註: 如未能通過 A－G 項之檢查，系統會隨即停止往後之檢查，並發出回覆檔案顯示錯誤原因。

4.3.3 分拆上載 XML 檔案

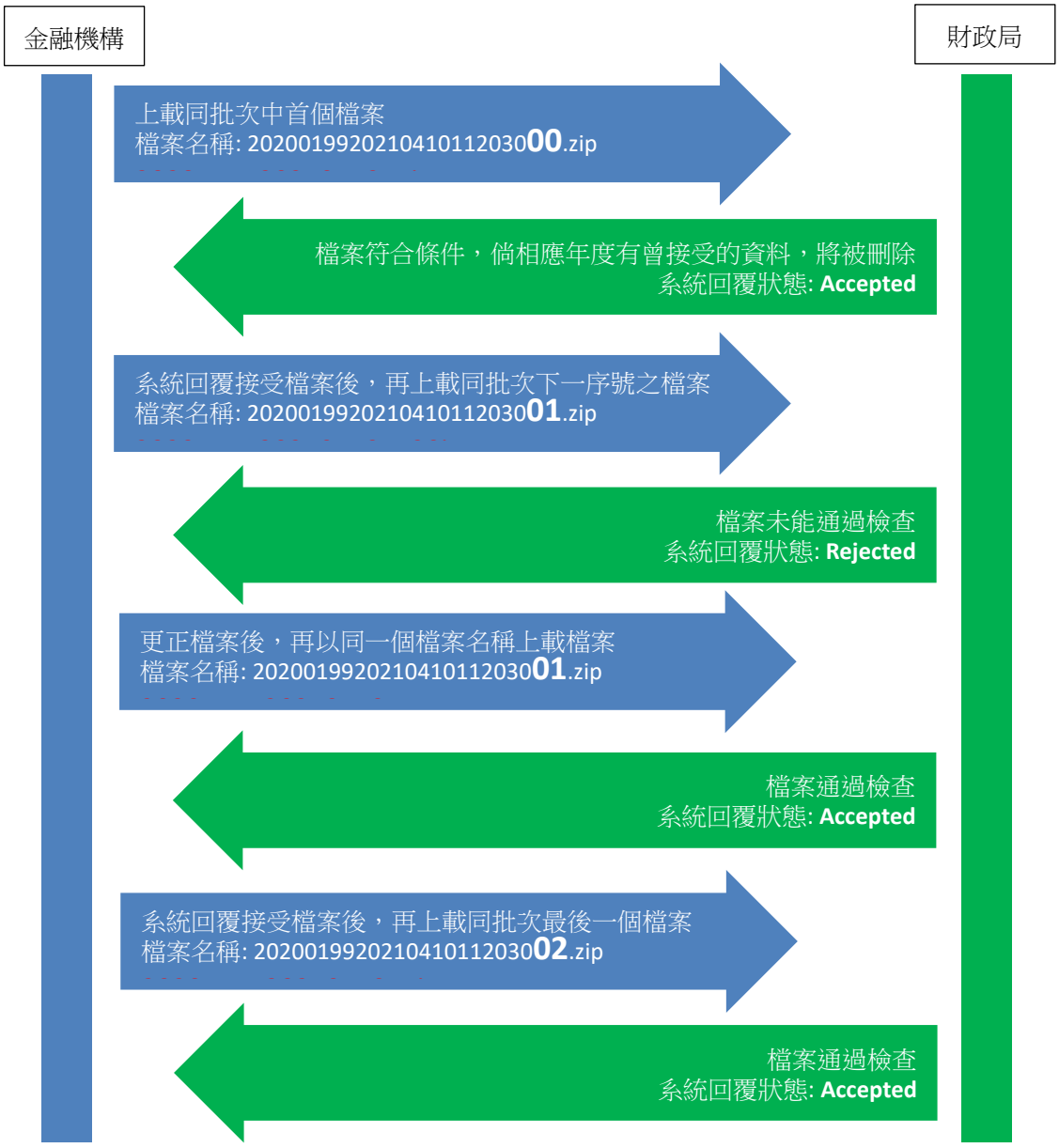
在報送期內，如金融機構須要報送的帳戶資料數量多於 60 萬筆，或因業務需要而不能一次性上載資料，請將資料分拆上載至系統。

分拆上載 XML 資料的規則/要求如下：

1. 分拆上載 XML 檔案僅適用於報送期限內資料；
2. 分拆後每個檔案大小須小於 800MB；
3. 同批次的 XML 檔案名稱除最後 2 位數字外須完全一致。而每個檔案名稱最後 2 位數字的序號須按順序命名(序號由 00 開始增加至 99)，以遞交 2020 年度的資料為例(同批次檔案被分拆為 3 個檔案)，檔案名稱分別如下：

   2020019920210410112030**00**.xml (0199 為金融機構之 AEOI ID)
   2020019920210410112030**01**.xml
   2020019920210410112030**02**.xml
4. 每個 XML 檔案須以新增記錄(New Data)類型編制，且須符合 AEOI XML Schema 規範；
5. 每個檔案須獨立進行電子簽署及加密等處理，從而得到對應的.zip 檔案(即每個 zip 檔案內均含 xml 資料檔案及其 Key 檔案)；
6. 同批次首個上載之檔案序號必須為 **00**
   (如:2020019920210410112030**00**.zip)；
7. 同一批次檔案必須按順序逐一上載，當系統處理完成並回覆接受檔案後，方可上載下一序號之檔案；
8. 同一批次的首個檔案(如:2020019920210410112030**00**.zip)如符合條件，相應資料年度曾遞交的資料將被刪除(請參閱“4.3.2 期限內資料的更正”)，如要清除上一批次已接受的資料，金融機構只須上載另一批次的首個檔案，即檔案名稱中的日期或時間部份與已提交的不同(如:202001992021**041112200000**.zip)；
9. 除同批次首個上載的檔案外，其後上載的檔案倘被系統拒絕，系統並不會刪除先前已接受的資料，金融機構只須以同一檔案名稱重新上載正確的資料即可。

以分拆檔案報送期限內資料例子:



4.4 期限後報送

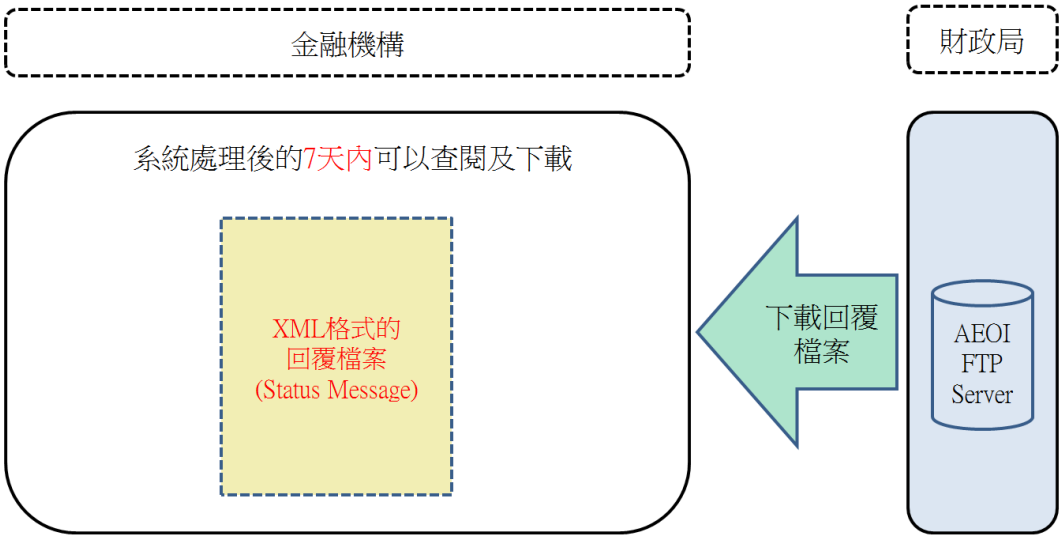
法定報送期後，倘發現已報送的金融帳戶信息有誤或遺漏，金融機構祇須上載相應新增/更正的帳戶資料。於文件夾內金融機構可上載多個新增、更正或刪除帳戶資料的檔案。系統檢查檔案名稱符合格式要求後，將按上載檔案的名稱所顯示的日期及時間順序處理。倘於文件夾內上載的多個檔案中有檔案未能通過檢查時，系統將按順序處理其他檔案。

如金融機構須要新增、更正或刪除帳戶的資料多於 60 萬筆，金融機構可於文件夾內上載多個不多於 60 萬筆資料的檔案，以完成有關操作。

5. 查閱報送狀態

5.1 查閱回覆檔案

各金融機構上載檔案後，系統會定時處理有關資料，金融機構可於系統完成處理後使用 FTPs 軟件登入系統專用伺服器，進入相關回覆文件夾內，下載有關的回覆檔案，回覆檔案以 XML 格式存放(詳情請參閱 AEOI Status Message User Guide)，系統將保留有關之回覆檔案七天。



5.2 查閱系統內有效記錄總數

系統成功處理金融機構上載的檔案後，會將載有系統內有效記錄總數的檔案存放到對應的回覆文件夾(/OUT_Production 或/OUT_Production_After 等等)，例如：檔案上載到 IN_Production 後，有效記錄總數資料將對應存放到 Out_Production)，有關資料經過加密及壓縮處理，檔案名稱為：YYYY_ AccountReportCount.zip(YYYY 為資料所屬年度)。金融機構可以使用財政局提供之輔助軟件對檔案進行解壓及解密，有關軟件及相關說明文檔可於財政局網站 www.dsf.gov.mo 下載。

– – 完 – –

附錄一 簽署及加密說明

***Step:* 1 – Sign the XML File**
***File Naming Convention:* YYYYXXXXYYYYMMDDHHMMSS00.xml**

Step description:

- Prepare the data using XML element prefixes. Do not use the default namespaces.
- To generate the digital signature[1], the XML file is processed by a "one–way hashing" algorithm to generate a fixed length message digest.
- Depending on the tool used to perform the digital signature, a different type of canonicalization method may be required. The following methods are acceptable:
  - <Canonicalization Method Algorithm="http://www.w3.org/2001/10/xmlexc–c14n#"/>
  - <Canonicalization Method Algorithm="http://www.w3.org/TR/2001/RECxml–c14n–20010315"/>
- It is required that the XML file be signed by first creating a SHA2–256[2] hash. The sending Financial Institution will then create an RSA digital signature using the 2048–bit private key from eSignTrust.
- After validating the schema, digitally sign the XML file using W3C Recommendation XML Signature Syntax and Processing (Second Edition)[3] "enveloping" signature.
- Use the digital signature "enveloping" type. The "enveloped and detached" types will cause the transmission to fail. The file name is "YYYYXXXXYYYYMMDDHHMMSS00.xml". The file name and extension are case sensitive and any variation in file name or format will cause the transmission to fail.

1. Digital Signature Standard (DSS) (FIPS 186–4), July 2013, nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186–4.pdf

2. Secure Hash Standard (SHS) (FIPS 180–4), March 2012, csrc.nist.gov/publications/fips/fips180–4/fips–180–4.pdf

3. XML Signature Syntax and Processing (Second Edition), June 2008, http://www.w3.org/TR/xmldsig–core/

***Step:* 2 – Compress the XML File**
***File Naming Convention:* YYYYXXXXYYYYMMDDHHMMSS00.zip**

Step description:

- Ensure "zip" is the file extension used by the compression tool or library.
- Ensure the file is compressed using the deflate compression algorithm.

Summary:

- The file name is "YYYYXXXXYYYYMMDDHHMMSS00.zip". The file is case sensitive and any variation in file name or format will cause the transmission to fail.
- Note: The current supported compression is ZIP compression using the standard Deflate compression method.

***Step:* 3 – Encrypt the XML File with AES 256 Key**
***File Naming Convention:* YYYYXXXXYYYYMMDDHHMMSS00**

Step description:

- After compression, encrypt the file "YYYYXXXXYYYYMMDDHHMMSS00.zip" using the AES–256 cipher with a randomly generated "one–time use" AES key.
- There are several steps necessary to perform AES encryption. The following agreed settings should be used to maintain compatibility:
  - Cipher Mode: CBC (Cipher Block Chaining)
  - Salt: No salt value
  - Initialization Vector (IV): 16 byte IV. The IV must, for the FI performing the encryption, be random and unique for every encryption.
  - Key Size: 256 bits / 32 bytes – the key size should be verified. Moving the key across operating systems can affect the key size.
  - Encoding: None. There can be no special encoding. The file will contain only the raw encrypted bytes.
  - Padding: PKCS#7 version 1.5
- The AES encrypted file name is "YYYYXXXXYYYYMMDDHHMMSS00". The file is case sensitive and any variation in file name or format will cause the transmission to fail.
- Additional information regarding the AES–256 encryption algorithm and keys can be found in:
  - NIST Special Publication 800–57: Recommendation for Key Management – Part 1: General (Revision 3)
  - Advanced Encryption Standard (FIPS 197), November 2001

***Process:* Validate Certificate**
***Step:* 4a – Encrypt the AES Key and IV with Public Key of Recipient**
***File Naming Convention:* N/A**

Step description:

- To validate the certificate:
  1. Verify the certificate chain.
  2. Check the revocation status of the certificate chain. There are two methods:
  - Retrieve a Certificate Revocation List (CRL) or
  - Send an Online Certificate Status Protocol (OCSP) query to a Certificate Authority designated responder

Process: **Encrypt the AES Key**
Step: **4b – Encrypt the AES Key and IV with Public Key of FSB**
File Naming Convention: **YYYYXXXXYYYYMMDDHHMMSS00_Key**

Step description:

- After validating the certificate, use the public key from FSB's certificate to encrypt the 32 byte AES 256 key concatenated with the 16 byte IV. The encrypted value must be 48 bytes in length.
- The public key encryption uses the standard RSA algorithm. There are several steps necessary to perform AES encryption. The following agreed settings should be used to maintain compatibility:
  - Padding: PKCS#1 version 1.5
  - Key Size: 2048 bits
- The encrypted file name is "YYYYXXXXYYYYMMDDHHMMSS00_Key".

Summary:

- There will be two encrypted files. The files are case sensitive and any variation in file name or format will cause the transmission to fail:
  1. Symmetric encryption – the AES 256 encrypted XML file name is "YYYYXXXXYYYYMMDDHHMMSS00"
  2. Asymmetric encryption – the public key encrypted AES 256 key file name is "YYYYXXXXYYYYMMDDHHMMSS00_Key"

Step: **5 – Create the transmission file (data packet)**

The two files to be contained in a data packet are:

File Name	Description
YYYYXXXXYYYYMMDDHHMMSS00	Encrypted XML using a randomly generated one–time use key
YYYYXXXXYYYYMMDDHHMMSS00_Key	Key encrypted using FSB's public key

The data packet will be named:

File Name	Description
YYYYXXXXYYYYMMDDHHMMSS00.zip	Transmission file to be sent through FTPs

For example: 20170012201803151230200 0.zip

附錄二 簽署及加密代碼示例

- XML Signature Syntax and Processing (Second Edition)
  https://www.w3.org/TR/xmldsig–core/

- C# XML Signature
  https://msdn.microsoft.com/en–us/library/system.security.cryptography.xml.signedxml(v=vs.110).aspx

- Java XML Signature
  http://docs.oracle.com/javase/8/docs/technotes/guides/security/xmldsig/XMLDigitalSignature.html

- C# AES Encryption
  https://msdn.microsoft.com/en–us/library/system.security.cryptography.aes(v=vs.110).aspx

- C# RSA(Certificate) Encryption
  https://msdn.microsoft.com/en–us/library/system.security.cryptography.rsacryptoserviceprovider(v=vs.110).aspx

- Java Encryption
  http://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#SimpleEncrEx